THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of establishing a common shared key between a pair of correspondents, said method comprising the steps of exchanging messages between the correspondents and including identification information in said messages, said information being identifiable to one or other of said correspondents to thereby establish said common key.

2. A method as defined in claim 1, including the steps of providing identities of the sender and the receiver including a flow number in a message to be signed.

3. A method as defined in claim 1, said step of exchanging messages being based on a STS-MAC Protocol.

4. A method as defined in claim 3, including the step of transmitting the sender's certificate in a first flow to thereby minimize an on-line UKS attack against a recipient.

5. A method as defined in claim 1, including the step of providing the identities of the correspondents in a key derivation function rather than a signed message.

6. A method as defined in claim 1, said exchange of messages being based on an STS-ENC Protocol.

7. A method as defined in claim 1, said exchange of messages being based on an STS-MAC Protocol.